AO 91 (Rev. 11/11) Criminal Complaint (Rev. by USAO on 3/12/20) ☐ Original ☐ Duplicate Original

UNITED STATES DISTRICT COURT

for the

Central District of California

UNITED STATES OF AMERICA,

v.

Daniel Andres ARAVENA OLIVA,

Defendant.

Case No. 2:24-MJ-05045-DUTY

CRIMINAL COMPLAINT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the dates of March 21, 2024, to April 5, 2024, in the county of Los Angeles in the Central District of California, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. § 2251(a), (e)	Attempted production of child pornography

This criminal complaint is based on these facts:

Please see attached affidavit.

☒ Continued on the attached sheet.

/s/ Paley Mao
Complainant's signature

Paley Mao, Special Agent
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: August 21, 2024

Alicia G. Rosenberg
Judge's signature

City and state: Los Angeles, California

Hon. Alicia G. Rosenberg, U.S. Magistrate Judge
Printed name and title

AUSA: Jeremiah Levine

AFFIDAVIT

I, Paley Mao, being duly sworn, declare and state as follows:

I. BACKGROUND OF SPECIAL AGENT PALEY MAO

1. I have been employed as a Special Agent ("SA") of the U.S. Department of Homeland Security, Homeland Security Investigations ("HSI"), since July 2023, and am currently assigned to the Child Exploitation Task Force, where I investigate criminal violations relating to child exploitation and child pornography, illegal production, distribution, receipt and possession of child pornography, in violation of 18 U.S.C. § 2252A, among other violations. While employed by HSI, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I have gained experience through training and everyday work relating to conducting these types of investigations. I have received training in the domain of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. Prior to my employment with HSI, I was a counterintelligence special agent with the Air Force Office of Special Investigations for approximately three years. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. § 2251, 2252, 2252A, 2242, and 2243, and I am authorized by law to request an arrest warrant.

II. PURPOSE OF AFFIDAVIT

2. This affidavit is made in support of a criminal complaint against and arrest warrant for Daniel Andres ARAVENA OLIVA ("ARAVENA") for violations of 18 U.S.C. § 2251(a), (e) (attempted production of child pornography).

3. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested complaint and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

III. SUMMARY OF PROBABLE CAUSE

4. Minor Victim 1 ("MV-1") is a minor female living in Glendora, California. Early in 2024, MV-1's mother and school officials reported illegal conduct to the Glendora Police Department. Specifically, they reported to GPD that MV-1 was engaged in inappropriate conversations with ARAVENA via Google Slides and Zoom chat. State search warrants executed by Glendora Police Department for ARAVENA's Google Slides and Zoom chat accounts revealed that he had sexually explicit conversations with MV-1. The text of the conversations showed that ARAVENA had directed MV-1 to self-produce child

pornography. The child pornographic images themselves had been deleted.

5. ARAVENA also told MV-1 that he would travel to see her and stay near her home.

6. On August 19, 2024, ARAVENA landed at Los Angeles International Airport ("LAX"). A consent search of his phone revealed sexually explicit images of MV-1. He admitted knowing that MV-1 was 14 years old. He also admitted having sexually explicit video chats with MV-1, and that he came to Los Angeles, CA in order to see MV-1.

IV. BACKGROUND ON CHILD EXPLOITATION OFFENSES, COMPUTERS, THE INTERNET, AND DEFINITION OF TERMS

7. In this affidavit, the terms "minor," "sexually explicit conduct," "visual depiction," "producing," and "child pornography" are defined as set forth in 18 U.S.C. § 2256. The term "computer" is defined as set forth in 18 U.S.C. § 1030(e)(1).

8. Based upon my training and experience in the investigation of child pornography, and information related to me by other law enforcement officers involved in the investigation of child pornography, I know the following information about the use of computers with child pornography:

a. Computers and Child Pornography. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. Child pornographers can now produce both still and moving images

directly from a common video camera and can convert these images into computer-readable formats. The use of digital technology has enabled child pornographers to electronically receive, distribute, and possess large numbers of child exploitation images and videos with other Internet users worldwide.

b. File Storage. Computer users can choose their method of storing files: either on a computer's hard drive, an external hard drive, a memory card, a USB thumb drive, a smart phone or other digital media device, etc. (i.e., "locally") or on virtual servers accessible from any digital device with an Internet connection (i.e., "cloud storage"). Computer users frequently transfer files from one location to another, such as from a phone to a computer or from cloud storage to an external hard drive. Computer users also often create "backup," or duplicate, copies of their files. In this way, digital child pornography is extremely mobile and such digital files are easily reproduced and transported. For example, with the click of a button, images and videos containing child pornography can be put onto external hard drives small enough to fit onto a keychain. Just as easily, these files can be copied onto compact disks and/or stored on mobile digital devices, such as smart phones and tablets. Furthermore, even if the actual child pornography files are stored on a "cloud," files stored in this manner can only be accessed via a digital device. Therefore, viewing this child pornography would require a computer, smartphone, tablet, or some other digital device that allows the user to access and view files on the Internet.

c. Internet. The term "Internet" is defined as the worldwide network of computers – a noncommercial, self-governing network devoted mostly to communication and research with roughly 500 million users worldwide. The Internet is not an online service and has no real central hub. It is a collection of tens of thousands of computer networks, online services, and single user components. In order to access the Internet, an individual computer user must use an access provider, such as a university, employer, or commercial Internet Service Provider ("ISP"), which operates a host computer with direct access to the Internet.

d. Internet Service Providers. Individuals and businesses obtain access to the Internet through ISPs. ISPs provide their customers with access to the Internet using telephone or other telecommunications lines; provide Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs' servers; remotely store electronic files on their customer's behalf; and may provide other services unique to each particular ISP. ISPs maintain records pertaining to the individuals or businesses that have subscriber accounts with them. Those records often include identifying and billing information, account access information in the form of log files, e-mail transaction information, posting information, account application information, and other information both in computer data and written record format.

e. IP Addresses. An Internet Protocol address ("IP Address") is a unique numeric address used to connect to the Internet. An Ipv4 IP Address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). In simple terms, one computer in a home may connect directly to the Internet with an IP Address assigned by an ISP. What is now more typical is that one home may connect to the Internet using multiple digital devices simultaneously, including laptops, tablets, smart phones, smart televisions, and gaming systems, by way of example. Because the home subscriber typically only has one Internet connection and is only assigned one IP Address at a time by their ISP, multiple devices in a home are connected to the Internet via a router or hub. Internet activity from every device attached to the router or hub is utilizing the same external IP Address assigned by the ISP. The router or hub "routes" Internet traffic so that it reaches the proper device. Most ISPs control a range of IP Addresses. The IP Address for a user may be relatively static, meaning it is assigned to the same subscriber for long periods of time, or dynamic, meaning that the IP Address is only assigned for the duration of that online session. Most ISPs maintain records of which subscriber was assigned which IP Address during an online session.

f. IP Address - Ipv6. Due to the limited number of available Ipv4 IP addresses, a new protocol was established using the hexadecimal system to increase the number of unique IP addresses. An Ipv6 consists of eight sets of combination of

four numbers 0-9 and/or letters A through F. An example of an Ipv6 IP address is 2001:0db8:0000:0000:0000:ff00:0042:8329.

g. The following definitions:

i. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

ii. "Chat room," as used herein, refers to the ability of individuals to meet in one location on the Internet in order to communicate electronically in real-time to other individuals. Individuals may also have the ability to transmit links to electronic files to other individuals within the chat room.

iii. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

iv. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where: (a) the production of the visual depiction involved the use of a minor

engaged in sexually explicit conduct; (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

v. "Cloud-based storage," as used herein, is a form of digital data storage in which the digital data is stored on remote servers hosted by a third party (as opposed to, for example, on a user's computer or other local storage device) and is made available to users over a network, typically the Internet. Users of such a service can share links and associated passwords to their stored files with other traders of child pornography in order to grant access to their collections. Such services allow individuals to easily access these files through a wide variety of electronic devices such as desktop and laptop computers, mobile phones, and tablets, anywhere and at any time. An individual with the password to a file stored on a cloud-based service does not need to be a user of the service to access the file. Access is typically free and readily available to anyone who has an Internet connection.

vi. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, other

mobile phones, and other mobile devices. *See* 18 U.S.C. § 1030(e)(1).

vii. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, "thumb," "jump," or "flash" drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

viii. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

ix. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of

hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

x. "Encryption" is the process of converting data into a code in order to prevent unauthorized access to the data.

xi. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

xii. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

xiii. An "Internet Protocol address" or "IP address," as used herein, refers to a unique numeric or

alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers ("ISPs") control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

xiv. "Log files" are records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.

xv. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

xvi. "Mobile applications," as used herein, are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game.

xvii. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

xviii. "Remote computing service," as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

xix. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

xx. A "storage medium" or "storage device" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, "thumb," "jump," or "flash" drives, CD-ROMs, and other magnetic or optical media.

xxi. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of

conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

xxii. A "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

V. STATEMENT OF PROBABLE CAUSE

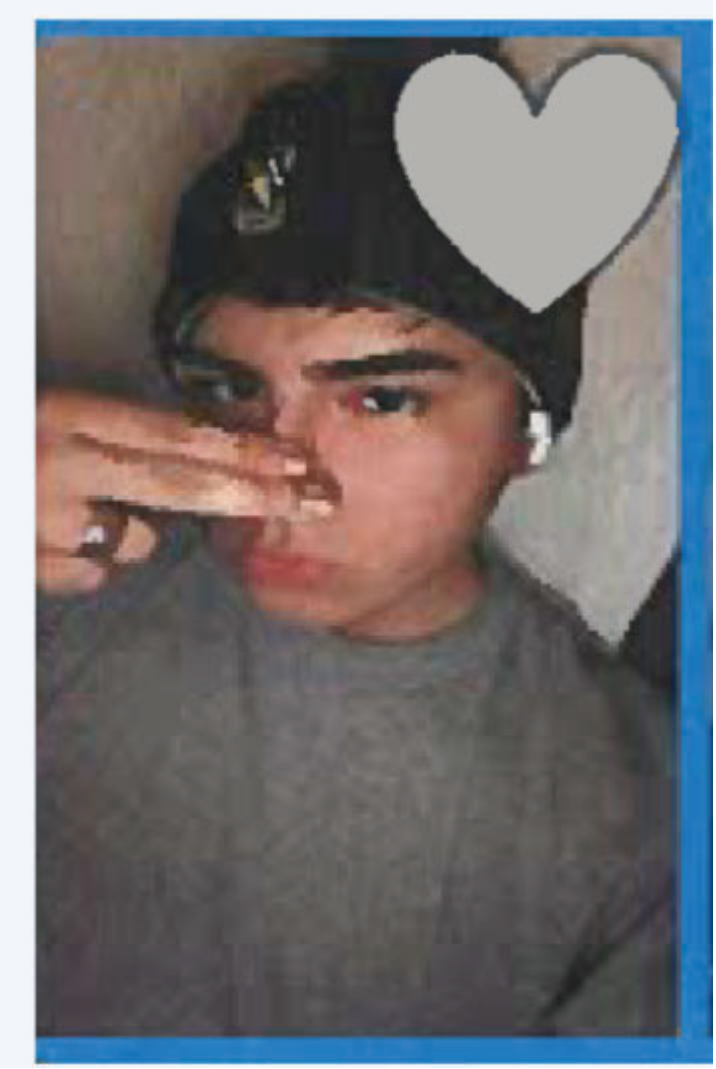
9. Based on my review of law enforcement reports, conversations with other law enforcement agents, and my own knowledge of the investigation, I know the following:

A. Initial Glendora PD Referral

10. On or about April 9, 2024, GPD responded to MV-1's school in Glendora, California. GPD met with MV-1's mother and school officials, who reported they had discovered a non-school affiliated email account (1danielandres0@gmail.com) was communicating with MV-1's school email account via Google Slides.[1] The school official checked MV-1's Google Slides account and discovered photographs and messages shared between MV-1 and 1danielandres0@gmail.com. One of the photographs showed an arm with a wristband bearing the name "Daniel Aravena Oliva." Another photograph showed a Zoom Chatroom ID number (875 1846 2151). The slides also contained "selfie" style

[1] Google Slides is a free web-based program for creating presentations.

photographs of ARAVENA. Here is a selfie photo that ARAVENA sent to MV-1:



11. When interviewed by GPD, MV-1 identified the individual she communicated with as Daniel Andres ARAVENA OLIVA. MV-1 informed GPD that she and ARAVENA were in a mature relationship. MV-1 stated they met on the online game Roblox. MV-1 confirmed ARAVENA directed her to take sexually explicit photographs/videos of herself to send to him. ARAVENA took screenshots and stated to MV-1 he was saving the content for further viewing. MV-1 said she also frequently spoke with

ARAVENA via live Zoom calls where she exposed herself a lot starting in approximately December 2023.

12. MV-1 provided the following social media accounts and email accounts for ARAVENA:

a. Emails: 1danielandres0@gmail.com, nanineitor3@gmail.com, dachellemagicky@gmail.com

b. Roblox accounts: vextzo, sp9c65

13. Glendora PD Detective Daniel Gigliobianco served search warrants to Google, Zoom, and Roblox to further identify ARAVENA. The search warrant returns disclosed the following information:

a. Google's warrant return indicated the user for "1danielandres0@gmail.com" had an internet protocol (IP) address located in Santiago, Chile.

b. Roblox's warrant return indicated the user for Roblox usernames "vextzo" and "sp9c65" had an IP address located in Santiago, Chile. Roblox only provided a one-sided conversation of the messages sent from ARAVENA.

c. Zoom's warrant return disclosed thousands of messages between ARAVENA and MV-1. No child sexual abuse material content was recovered; it appeared ARAVENA deleted all of the visual content MV-1 sent to him. However, many of the messages were sexual in nature and described the videos and photographs MV-1 sent ARAVENA, and recorded ARAVENA's directions to MV-1 for different poses and sex acts during live video calls. ARAVENA's messages to MV-1 included the following

verbatim quotes, which took place between approximately March 21, 2024, and April 5, 2024:

d. Yes my little ilegal slut

e. So show me ur asshole to prove it

f. Yes I took screenshot

g. Show me ur pussy and Ill see if u look like a mommy

h. Show me ur clit

i. Next year I'll go to California

j. I'll sniff your asshole after you take a shit

k. My little dirty slut I'll fuck you so fucking much every single day

l. Get closer to the camera show me that stinky asshole

m. Is that poop bb or blood

n. Put your finger in

o. And If I feel lazy I'll just wear a condom so we don't have to worry about if u shit on my dick

14. Following the school's report to GPD, the school blocked ARAVENA's email address from communicating with MV-1's school email address. MV-1's mother confiscated her electronic devices and means of communicating with ARAVENA. ARAVENA began to create burner emails to try and reach MV-1. The email addresses were various combinations of ARAVENA's and MV-1's names and initials. ARAVENA went as far as to contact MV-1's family and school on a nearly daily basis.

15. On or about June 26, 2024, MV-1's aunt spoke with ARAVENA on the phone. The aunt recorded the conversation and provided it to GPD. The aunt informed ARAVENA that the photographs and videos of MV-1 were child pornography and illegal, and that ARAVENA could go to prison. ARAVENA acknowledged that child pornography was illegal and that he could go to prison. The aunt informed ARAVENA that law enforcement had been notified of ARAVENA's actions, but ARAVENA continued to request to speak with MV-1.

16. On or about August 14, 2024, Det. Gigliobianco received additional Google Slides from MV-1's school that the school recovered from MV-1's Google Slides account. One of the slides contained a photograph of a flight itinerary booked for ARAVENA. The reservation number and passport number were redacted. The inbound flight was LATAM Airlines flight LA532 on August 19, 2024, arriving at John F. Kennedy International Airport ("JFK"), New York, NY; and the outbound flight was LATAM Airlines flight LA533 on August 28, 2024, departing from JFK, New York, NY.

B. Identifying Subject's Travel Itinerary

17. On or about August 15, 2024, I conducted a law enforcement database search and did not find any flight reservations for ARAVENA. I was able to identify an ESTA application ARAVENA submitted in approximately June 2024. ARAVENA provided the following identifiers on his ESTA application, among others:

a. Name: Daniel Andres ARAVENA OLIVA

b. Date of Birth: 08/10/2003

c. Email Address: nanineitor3@gmail.com

d. U.S. Address: [omitted by affiant] La Verne, CA

18. The above identifiers were all corroborated either by MV-1's prior interview, or by ARAVENA's messages to MV-1 via Zoom. Det. Gigliobianco was able to positively identify ARAVENA as the individual who was communicating with MV-1 by comparing ARAVENA's ESTA application photo and the "selfie" style photographs from MV-1's Google Slides.

19. I also noted ARAVENA listed a United States address of [street address omitted by affiant] La Verne, CA, on his ESTA application. Chat logs indicate that MV-1 previously provided her home address to ARAVENA and that ARAVENA stated he was going to stay on [address omitted by affiant] in La Verne to be close to MV-1.

20. On or about August 19, 2024, I submitted a customs summons to Airbnb to determine whether ARAVENA's U.S. address was an Airbnb, and if so, who the customer was. On or about August 20, 2024, Airbnb provided the following reservation information for ARAVENA's U.S. address for the period of August 20, 2024, through September 5, 2024:

Name: Daniel Aravena

Email: nanineitor3@gmail.com

21. On or about August 16, 2024, I coordinated with HSI JFK. HSI JFK was able to locate updated reservations for ARAVENA. ARAVENA's new flight information indicated he was set to arrive at LAX aboard LATAM flight LA602, from Santiago,

Chile, on August 20, 2024. ARAVENA was scheduled to depart LAX to return to Santiago, Chile, aboard LATAM flight LA601 on September 6, 2024.

C. Arrest and Interview of the Subject

22. On or about August 16, 2024, Det. Gigliobianco informed me he had obtained a state arrest warrant for ARAVENA for possession of child pornography, production of child pornography, enticement of a minor, and harassing phone calls and communications.[2]

23. On or about August 20, 2024, ARAVENA arrived at LAX aboard LATAM flight LA602. Customs and Border Protection Officers ("CBPOs") conducted a secondary interview of ARAVENA. ARAVENA informed the CBPOs that he did not know anyone in the United States and that he was here on tourism. ARAVENA stated he would be staying in La Verne, CA.

24. Following the CBPOs' interview of ARAVENA, I requested to inspect ARAVENA's cell phone. ARAVENA voluntarily provided me his phone password and signed a consent to search form. ARAVENA spoke English, but to ensure he understood what he was signing, the CBPOs also informed him of the consent form in Spanish. In ARAVENA's "Deleted Photos" folder, I located sexually explicit videos and photographs of a female.[3] Some of

---

[2] He also informed me that he had applied for a state warrant to search any digital devices ARAVENA had when he landed. That warrant application was denied, and the judge conveyed that Det. Gigliobianco should reapply once he had in custody the specific devices he wanted to search.

[3] The "Deleted Photos" folder on iPhones retained deleted photos for approximately 30 days before they are permanently

the photos had a female's face; Det. Gigliobianco was able to visually identify the female as MV-1.

25. Following my inspection of ARAVENA's phone, Det. Gigliobianco placed ARAVENA under arrest pursuant to the state arrest warrant. Det. Gigliobianco and Glendora PD Detective Mykel Tso interviewed ARAVENA at HSI Los Angeles International Airport.

26. I observed the recorded, post-Miranda interview of ARAVENA conducted by Det. Gigliobianco and Det. Tso. ARAVENA disclosed the following information:

a. ARAVENA knew MV-1 was 14 years of age;

b. ARAVENA came to the United States because he could no longer communicate with MV-1, and wanted MV-1 to know he had not forgotten her;

c. ARAVENA stated he intended to stay in La Verne, CA;

d. ARAVENA stated he may have been too nervous to have sex with MV-1 upon meeting her in person, but would have done so if MV-1 agreed to have sex;

e. ARAVENA asserted MV-1 was the first to send a sexually explicit photograph;

f. ARAVENA acknowledged he was the individual sending the messages provided in the Zoom search warrant return;

---

deleted. The deleted videos and photographs I identified had approximately 29 days left before permanent deletion, indicating ARAVENA deleted them approximately the day of his flight to the United States.

g. ARAVENA acknowledged he had called MV-1 his "little ilegal [sic] slut";

h. ARAVENA admitted to sexual conduct with MV-1 via video calls;

VI. TRAINING & EXPERIENCE ON INDIVIDUALS WHO HAVE A SEXUAL INTEREST IN CHILDREN

27. Based on my training and experience, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned that there are certain characteristics common to individuals with a sexual interest in children and images of children:

a. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, in person, in photographs, or in other visual media; or from literature describing such activity.

b. Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides, and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower

the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who have a sexual interest in children or images of children sometimes possess hard copies of child pornography, such as pictures, films, video tapes, magazines, negatives, photographs, etcetera. As digital technology has developed, individuals with a sexual interest in children or images of children have become much more likely to maintain child pornography in digital or electronic format, stored either on digital devices or in remote storage locations on the Internet. Regardless of whether these individuals collect their child pornography in hard copy or digital format, they may maintain their child pornography for a long period of time, even years. They usually maintain these collections in a safe, secure, and private environment, such as their homes, vehicles, or nearby, so they can view the child pornography at their leisure. These collections are typically highly valued.

d. Individuals who have a sexual interest in children or images of children also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors and collectors; may conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

e. Individuals who have a sexual interest in children or images of children prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

VII. CONCLUSION

28. For all the reasons described above, there is probable cause to believe that ARAVENA has committed violations of 18 U.S.C. § 2251(a), (e) (attempted production of child pornography).

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 21st day of August, 2024.

Alicia G. Rosenberg

HONORABLE ALICIA G. ROSENBERG
UNITED STATES MAGISTRATE JUDGE